SECURITY AND RELIABILITY OF RATIONAL PLAYERS IN DISTRIBUTED CONSENSUS

Kehelwala Gamaralalage Janani Hansika Kehelwala

189329L

Degree of Master of Science

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

May 2021

SECURITY AND RELIABILITY OF RATIONAL PLAYERS IN DISTRIBUTED CONSENSUS

Kehelwala Gamaralalage Janani Hansika Kehelwala

189329L

Dissertation submitted in partial fulfillment of the requirements for the degree of MSc in Computer Science specializing in Security Engineering

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2021

DECLARATION

Candidate:

I declare that this is my own work and this dissertation does not incorporate, without acknowledgment, any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where the acknowledgment is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

-     - - - - - - - - - - - - - - - - -

K. G. J. H. Kehelwala   Date

Supervisor:

The above candidate has carried out research for the Masters Dissertation under my supervision.

-     - - - - - - - - - - - - - - - - -

Dr. C. D. Gamage   Date

ABSTRACT

Distributed ledgers and their applications in solving centralization problems in both financial and non-financial domains has been in the forefront of information security research since the emergence and the subsequent popularity of Blockchain. While the Proof of Work protocol has been successfully utilized for cryptocurrencies, the requirement for higher throughputs in non-financial domain based distributed ledgers favor alternate protocols whose consensus assumptions usually come with thresholds of Byzantine agents (faulty inputs) the consensus can withstand. Proof of Work is designed so that financial gain from conducting a successful attack is less than what honest participation would provide, eliminating any motivation an adversary might have to attack (within the context of direct gain). This assumption fails for non-financial solutions since resourceful malicious participants may exist where their gain may lie in manipulation of the distributed ledger or the order in which the transactions are recorded. A resourceful attacker could selectively convert rational agents to byzantine agents until the tolerance threshold is exceeded. Therefore, we propose that completeness assurance, and the overall reliability of distributed consensus requires rational and foresighted players to be sufficiently incentivized in affording costs of self-protection. We present a dynamic, complete, and imperfect information game to study the relationships between individual costs and utilities, tolerance threshold of the protocol and environment volatility in terms of exogenous attack probabilities, and observe conditions under which a mixed strategy equilibrium that preserves completeness would be stable. Our research extends existing literature by obtaining realistic resilience measures when considering rational player behavior in volatile environments, and provide a better understanding of mandatory security requirements that need to be implemented by a protocol designer for security in distributed consensus. We evaluate our proposed model using efficiency measurement concepts such as Price of Anarchy and Price of Malice, alongside learning methodologies such as regret matching and bounded rationality for extended insight. Our evaluations follow the theoretical predictions of the proposed model. Our results confirm reputation optimization to be capable of completeness assurance when the benefits are carefully assigned with consideration to tolerance threshold of the network. Our experiments also indicate that reputation optimization has attractive stability and convergence properties that are absent in other learning methodologies considered for evaluation.

Keywords: Incentive Compatibility, Mixed Strategy Equilibria, Social Trust Network, Bounded Rationality, Price of Malice, Game Theory, Distributed Consensus, Mechanism Design

DEDICATION

This dissertation is dedicated to my grandfather, Captain John Jayapala.
I hope there is peace. I hope you have found it.

ACKNOWLEDGMENTS

My gratitude goes to my supervisor, Dr. Chandana Gamage for providing continuous guidance throughout this endeavor. The expertise, resources and supervision provided by him were invaluable to the successful completion of this research. I would also like to thank Dr. Charith Chitraranjan and Dr. Indika Perera for the resources and guidance they provided in assessment and reviewing of literature.

Finally, my gratitude extends to my friends and family, whose support and patience has been a driving force throughout the duration of this effort.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
ABS	Agent Based Simulation
BFT	Byzantine fault tolerance
BGP	Byzantine Generals Problem
DES	Discrete Event Simulation
DMS	Dynamic Micro Simulation
DoS	Denial of Service
EFBP	El Farol Bar Problem
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Intellectual Property
MABS	Multi Agent Based Simulation
NFT	Non-fungible tokens
OOS	Object Oriented Simulation
PBFT	Practical Byzantine fault tolerance
PoA	Price of Anarchy
PoM	Price of Malice
PoW	Proof of Work
UNL	Unique Node List

LIST OF APPENDICES